UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,238	12/22/2000	David W. Grawrock	42390P9257	9482

8791 7590 08/27/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
DINH, MINH	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/747,238	GRAWROCK, DAVID W.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-28 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-28 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 December 2000 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 12/16/03. 12/17/03, 3/30/04, 4/2/04, 6/30/04, 7/2/04
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 have been examined.

Information Disclosure Statement

2. The following two publications have not been considered because their portions listed in the IDS filed 7/2/2004 do not match corresponding portions provided by the applicant:

- INTEL CORPORATION, "IA-64 System Abstraction Layer Specification", Intel Product Specification, Order Number 245359-001. (01/2000),1-112: only 41 pages of document (1-1—3-21) were provided, not 112 pages (1-112) as listed in the IDS.
- INTEL CORPORATION, "Intel IA-64 Architecture Software Developer's Manual", Volume 2: 1A-64 System Architecture, Order Number 245318-001, (01/2000),i, ii, 5.1-5.3, 11.1-11.8, 11.23-11.26: the notation listed in the IDS is for sections, not pages as provided (5-1—5-3, 11-1—11-8, 11-23—11-26).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 28 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Claim 28 recites the limitation "the initial event is a first power-up sequence after the first device is in communication with a second device". A first power-up sequence after the first device is in communication with the second device is not the initial power-up sequence. However, the specification discloses in both embodiments that generation of data is a one-time event and occurs in response to an initial event such as the initial power-up sequence (p. 5, 19-26 and p. 6, lines 1-5). Thus, the disclosure fails to enable one skilled in the art to make and use the claimed invention. The limitation is interpreted as "the initial event is the initial power-up sequence when the first device is in communication with a second device"

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier ("Applied Cryptography") in view of Menezes et al. ("Handbook of Applied Cryptography", Section 12.3). Schneier discloses a method comprising:

within a first device, generating a key-encryption key for permanent storage in a protected area of internal memory of the first device that prevents subsequent modification of the data (p. 176, 6th par., "Alice generates a key using a random-key generator."; p. 177, 2nd par., "However, since compromise ... be stored securely."); and

within the first device, producing a data key, which meets the limitation of a secret value, being a short term value generated in response to a periodic event (p. 177, 2nd par., "Once Alice and Bob both ... be changed as often.").

Schneier does not disclose that the secret value is a combination of both the data and a short-term value. Menezes discloses generating a secret value within the first device, the secret value being a combination of both the long-term value and a short-term value (p. 499, 1st par., "Here A could control ... time-variant parameter as noted above."). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Schneier method such that the secret value is a combination of both the long-term value and a short-term value, as taught by Menezes. The motivation for doing so would have been that a key derivation protocol which entirely avoids the use of an encryption function might offer potential advantages with respect to export restrictions (p. 499, 2nd par.).

7. Claims 2-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Menezes as applied to claim 1 above, and further in view of Ugon (4,795,893).

a. Regarding claims 2-3, Schneier and Menezes do not disclose that the periodic event includes a power-up sequence. Ugon discloses that electronic data processing units that include volatile memories loose all the information contained in these memories in the absence of electrical power (col. 1, lines 21-24). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier and Menezes to generate the short-term value in response to the power-up event because the previous short-term value has been lost in the absence of electrical power, as taught by Ugon.

b. Regarding claims 4-5, Schneier discloses transmitting the data to a second device prior to producing the secret value. Schneier does not disclose transmitting a first command from the second device to the first device prior to generating the data. However, Examiner takes Official Notice that an entity transmits a command to another entity requesting a key prior to the key being generated is conventional and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit a first command from the second device to the first device prior to generating the data since Examiner takes Official Notice that an entity transmits a command to another entity requesting a key prior to the key being generated is conventional and well known, and well known for the purpose of the other entity knowing when to generate the key and to whom the key is generated for.

c. Claim 6 is rejected for the same reason as claims 3-4 discussed above.

d. Regarding claim 7, Schneier does not disclose transmitting the short-term value to the second device prior to or concurrently with producing the secret value. Menezes discloses transmitting the short-term value to the second device prior to producing the secret value (p. 499, last par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Schneier method to transmit the short-term value to the second device prior to producing the secret value, as taught by Menezes. Please refer to motivation recited for generating a secret value within the first device, the secret value being a combination of both the long-term value and a short-term value as taught by Menezes in claim 1.

8. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Menezes as applied to claim 1 above, and further in view of Menezes ("Handbook of Applied Cryptography", Section 10.2). Schneier and Menezes do not disclose that the combination of claim 1 is a result produced by successively performing a hash operation on both the data and the short-term value. Menezes, in Section 10.2, discloses successively performing a hash operation (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claim 1 such that that the combination is a result produced by successively performing a hash operation on both the data and the short-term value, as taught by Menezes, in order to slow down attacks.

9. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pitchenik (6,397,328) in view of Menezes et al. ("Handbook of Applied Cryptography", Sections 12.2-12.3). Pitchenik discloses a method comprising:

generating a shared secret key, which meets the limitation of a long-term value, within a first device (fig. 2, step 100);

permanently storing the long-term value within a protected area of an internal memory of the first device (fig. 2, step 105);

providing the long-term value to a second device communicatively coupled to the first device (fig. 2, step 110).

Pitchenik does not disclose generating a short-term value within the first device, the short-term value being modified after each periodic event; providing the short-term value to the second device; and generating a secret value within the first device and the second device, the secret value being a combination of both the long-term value and the short-term value.

Menezes discloses a method for deriving a session key for each communications session between two entities using a long-term secret shared by the entities, the method comprising:

generating a short-term value within the first device, the short-term value being modified after each periodic event (p. 498, last par.);

providing the short-term value to the second device (p. 498, last par.); and

generating a session key, which meets the limitation of a secret value, within the first device and the second device, the session key being a combination of both the long-term value and the short-term value (p. 499, 1st par.).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Pitchenik method to include the steps of generating a short-term value within the first device, the short-term value being modified after each periodic event; providing the short-term value to the second device; and generating a session key within the first device and the second device, the session key being a combination of both the long-term value and the short-term value, as taught by Menezes. The use of session keys would limit available ciphertext (under a fixed key) for cryptanalyst attack (p. 494, 1st par.).

10. Claims 10-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pitchenik in view of Menezes as applied to claim 9 above, and further in view of Ugon.

a. Regarding claim 10, Pitchenik and Menezes do not disclose that the periodic event includes a power-up sequence. Ugon discloses that electronic data processing units that include volatile memories loose all the information contained in these memories in the absence of electrical power (col. 1, lines 21-24). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pitchenik and Menezes to generate the short-term value after the power-up event because the previous short-term value has been lost in the absence of electrical power, as taught by Ugon.

b. Regarding claim 11, Pitchenik does not disclose transmitting a first command from the second device to the first device prior to generating the long-term value, which is the shared secret key. However, Examiner takes Official Notice that an entity transmits a command to another entity requesting a key prior to the key being generated is conventional and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit a first command from the second device to the first device prior to generating the long-term value since Examiner takes Official Notice that an entity transmits a command to another entity requesting a key prior to the key being generated is conventional and well known, and well known for the purpose of the other entity knowing when to generate the key and to whom the key is generated for.

c. Regarding claim 12, Pitchenik further discloses that the long-term value is generated in response to an initial power-up sequence when the first device is in communication with the second device (fig. 2).

d. Claim 13 is rejected for the same reason as claim 11 discussed above.

11. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pitchenik in view of Menezes as applied to claim 9 above, and further in view of Menezes ("Handbook of Applied Cryptography", Section 10.2). Pitchenik and Menezes do not disclose that the combination of claim 9 is a result produced by successively performing a hash operation on both the data and the short-term value. Menezes, in Section 10.2, discloses successively performing a hash operation (p. 390, 2nd par.). It

would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of claim 1 such that that the combination is a result produced by successively performing a hash operation on both the data and the short-term value, as taught by Menezes, in order to slow down attacks.

12. Claims 15-16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (5,818,939) in view of Menezes ("Handbook of Applied Cryptography", Section 12.3) and Burns ("INTEL: Intel introduces new chipset for intel Pentium III processor-based performance PCs").

a. Regarding claims 15-16, Davis discloses a platform comprising:

a link (fig. 4, element 330);

an chipset coupled to the link (fig. 4, element 315); and

a cryptographic device, which meets the limitation of a trusted platform module (TPM), coupled to the link (fig. 4, element 335), the cryptographic coprocessor including

a package (fig. 4, element 335),

a asymmetric key generation unit contained within the packet to generate a shared secret key, which meets the limitation of a long term value (col. 5, lines 24-36; col. 6, lines 57-65); and

an internal memory contained within the package, the internal memory to permanently store the shared secret key (fig. 4, element 610) and to temporarily store a session key, which meets the limitation of a secret value (col. 6, lines 25-28).

Davis does not disclose an input/output control hub (ICH). Burns discloses a chipset comprising an ICH ("This revolutionary chipset architecture ... and a Firmware Hub"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis platform to use a chipset comprising an ICH, as taught by Burns. The ICH includes an Alert on LAN feature that allows a non-booting system to send a status update to the network administrator even when the microprocessor is not present.

Davis does not disclose that the asymmetric key generation unit generates a short-term value and the session key being a combination of the shared secret key and the short-term value. Menezes discloses a device that has a long-term shared secret key (p. 497, "Point-to-point key update ... a priori by two parties A and B"); and the device generates a short-term value and a session key, which meets the limitation of a secret value, the session key being a combination of the shared secret key and the short-term value (p. 499, 1st par., "Here A could control ... time-variant parameter as noted above."). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis platform such that the asymmetric key generation unit generates a short-term value and a secret value being a combination of the shared secret key and the short-term value, as taught by Menezes. The motivation for doing so would have been that a key derivation protocol which entirely avoids the use of an encryption function might offer potential advantages with respect to export restrictions (p. 499, 2nd par.).

b. Regarding claim 18, Davis further discloses that the asymmetric key generation unit includes a number generator (fig. 4, element 620).

13. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis ('939), Menezes and Burns as applied to claim 16 above, and further in view of Davis (5,949,881). Davis ('939) discloses that the cryptographic device transmits the shared secret key to the chipset over the link during manufacture of the platform (col. 5, lines 24-36; col. 6, lines 6-30); however, Davis does not disclose that the cryptographic device transmits the shared secret key to the ICH over the link during manufacture of the platform and transmits the short term value to the ICH over the link in response to a power-up sequence by the platform. Davis ('881) discloses a platform comprising a cryptographic device and an I/O controller, which meets the limitation of an ICH (fig. 1, elements 130 and 151). Davis further discloses that the cryptographic device and the I/O controller share a secret key (fig. 1; col. 3, lines 25-29), and that the cryptographic device generates and uses a session key, in addition to the symmetric key, to authenticate and activate the platform in response to a power-up sequence by the platform (fig. 2; col. 3, lines 13-16). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the platform of claim 16 such that the cryptographic device generates and uses a session key, in addition to the symmetric key, to authenticate and activate the platform in response to a power-up sequence by the platform, as disclosed by Davis in reference '881. Accordingly, the cryptographic device needs to transmit the long-term value to the ICH over the link during

manufacture of the platform and transmit the short-term value to the ICH over the link in response to a power-up sequence by the platform. The motivation for doing so would have been to reduce the value of a laptop computer in the event of its theft or loss and thus, in effect, would deter such theft and encourage its return in the event of loss (col. 1, lines 53-57).

14. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, Menezes and Burns as applied to claim 15 above, and further in view of Menezes ("Handbook of Applied Cryptography", Section 10.2). Davis, Menezes (Section 12.3) and Burns do not disclose that the cryptographic device comprise a cryptographic engine performing a successive hashing operation on both the long term value and the short term value to produce the secret value. Menezes, in Section 10.2, discloses a cryptographic engine performing a successive hashing operation on data (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the platform of claim 15 such that that the cryptographic device comprise a cryptographic engine performing a successive hashing operation on both the long term value and the short term value to produce the secret value, as taught by Menezes, in order to slow down attacks.

15. Claim 20, 22-23, 25-26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (5,819,939) in view of Menezes (Section 12.3).

a. Regarding claim 20, which is representative of claims 25-26, Davis discloses a device comprising:

an internal memory (fig. 4, element 610);

an asymmetric key generation unit to generate, in response to an initial event, a unique long-term value for permanent storage in a protected area of the internal memory (col. 5, lines 24-36; col. 6, lines 57-65).

Davis further discloses that the asymmetric key generation unit generates a session key, which meets the limitation of a secret value; however, Davis does not disclose that the asymmetric key generation unit generates, in response to a periodic event, a short-term value for storage in the internal memory and a cryptographic engine to produce the session key by combining both the long-term value and the short-term value. Menezes discloses a key generation unit for deriving a session key, which meets the limitation of a secret value, by generating, in response to a periodic event, a short-term value for storage in the internal memory (p. 498, last par.); and a cryptographic engine to produce the session key by combining both the long-term value and the short-term value (p. 499, 1st par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the Davis device such that the asymmetric key generation unit generates, in response to a periodic event, a short-term value for storage in the internal memory and a cryptographic engine to produce a secret value by combining both the long-term value and the short-term value, as taught by Menezes. The motivation for doing so would have been that a key derivation protocol

which entirely avoids the use of an encryption function might offer potential advantages with respect to export restrictions (p. 499, 2nd par.).

b. Regarding claims 22 and 28, Davis further discloses that the initial event includes an initial power-up sequence of the device when in communication with another device of the platform for which the secret value is generated to create one secure communication channel between the devices (col. 5, lines 24-36; col. 6, lines 6-30).

c. Regarding claim 23, Davis further discloses that the internal memory includes a non-volatile memory (fig. 4, element 610) and a volatile memory (fig. 4, element 615).

16. Claims 21 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Menezes as applied to claims 20 and 25 above, and further in view of Ugon. Davis and Menezes do not disclose that the periodic event includes a power-up sequence. Ugon discloses that electronic data processing units that include volatile memories loose all the information contained in these memories in the absence of electrical power (col. 1, lines 21-24). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Schneier and Menezes to generate the short-term value in response to the power-up event because the previous short-term value has been lost in the absence of electrical power, as taught by Ugon.

17. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Menezes as applied to claim 20 above, and further in view of Menezes (Section

10.2). Davis, Menezes (Section 12.3) do not disclose that the cryptographic engine performs successive hashing operations on the long-term value and the short-term value when combining the long-term value and the short-term value. Menezes, in Section 10.2, discloses a cryptographic engine performing a successive hashing operation on data (p. 390, 2nd par.). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of claim 20 such that that the cryptographic engine performs successive hashing operations on the long-term value and the short-term value when combining the long-term value and the short-term value, as taught by Menezes, in order to slow down attacks.

Conclusion

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Schweitzer et al. (5,850,450) discloses a method and apparatus for encryption key creation.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 703-306-5617. The examiner can normally be reached on Mon - Fri: 9:00 am - 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
8/16/04

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100